Virtual Identity Approaches Evaluation for Anonymous Communication in Cloud Environments

Ibrahim A.Gomaa[*§]
Department of Computers & Systems
[*] National Telecommunication Institute
[§] Helwan University, Cairo, Egypt

Emad Abd-Elrahman[*ϕ]
RST Department
[ϕ] Telecom SudParis, Evry, France

Mohamed Abid
IResCoMath Research Unit
National School of Engineers of Gabes, Tunisia

***Abstract*—Since the era of Cloud computing beginning, the Identity Management is considered as a permanent challenge especially for the hybrid IT environments that permit for many users' applications to share the same data center depending on servers' virtualization. This paper introduces a complete study about Identity forms in different domains and applications. Also, a performance evaluation of new approaches for Virtual Identity was done. Virtual Identity, a new terminology used in virtual environments, was introduced to enhance the anonymous communication in such types of complex networks. Based on the work analysis and motivations done through an online survey, two techniques were used to implement the Virtual Identity; Identity Based Encryption (IBE) and Pseudonym Based Encryption (PBE). Both techniques were validated using MIRACL library for security algorithms. In addition, the performance of both approaches was evaluated under different configurations and network conditions through OPNET Modeler. The results showed the impact of the number of cloud users and their locations (either local or remote) on the application response time in cloud environments using the proposed virtual identities. Moreover, Application Characterization Environment whiteboard was used to simulate the overall flow of data across different tiers from start to end of the application task for Virtual Identity creation. The results and outcomes for both methodologies showed that they are suitable paradigm for achieving high degree of security and efficiency in such sophisticated network access to many online services and applications.**

***Keywords*—Cloud Environments; Virtual Identity; Performance Evaluation and Security**

I. INTRODUCTION

Nowadays, the Internet is inundated by data generated from different sources. Users share personal details, opinions, videos, pictures and very often their identities for each service with public or even their friends. Identity-based service is registered either explicitly, by users who share their identities through social networks, or implicitly by access services through applications of portable devices.

Therefore, the virtualized services access management over the Internet is becoming a critical technology for maintaining privacy and performance especially after the transition to cloud computing. As keeping service provider assets secure is a suitable approach to all parties, anonymous communications between users and virtual service provider became critical issue for users to preserve their personal details.

Users continue to depend on the virtual environments for services' delivery and more individuals are using multiple types of devices to access those services, and applications, Hence, it is necessary hide who has access to the service. Often, users suffer from password bore, having to create and remember at least one password for each service/application. Adding to the challenges of cloud networking security is the increasingly wide range of structured and unstructured data that is exchanged across the network and the heterogeneity of devices used to access it from any place. The service provider must handle access from smart phones, tablets, PCs, and other form factors, often with different operating systems. Each device may equipped with access enterprise applications, mobile apps, social media, streaming video and traditional data each time in one access. Transactions mentioned before, creates a highly sophisticated environment in which the service provider must control how and who has access to what and when.

Table I summarizes and evaluates the four anonymous communication techniques that are available nowadays on the Internet.

This paper highlights the concept of anonymous communication by another way depending on the user identity to create virtual one for services anonymous login. A secure communication is established by creating this virtual identity using a triangle negotiation between the user, the Private Key Generator (PKG) and the service Provider (SP). This process is followed the Identity-Based Cryptography (IBC) methodology either using IBE or PBE techniques. Moreover, both techniques effects in Virtual Identity (V_{ID}) generation are simulated to confirm the solution feasibility for cloud service access. The rest of the paper is organized as follows: in Section 2, related work background and motivations will be presented and reviewed. Section 3 introduces identity in the cloud and virtual environments. Section 4 introduces the proposed V_{ID} mechanisms and its implementation using MIRACL library. Section 5 presents the performance evaluation using OPNET modeler and its results. Finally, Section 6 concludes the paper and future directions for anonymous communication using virtual identities in cloud environments is discussed.

TABLE I. ANONYMOUS COMMUNICATION TECHNIQUES

Parameter	anonymous communication familiar techniques			
	Private Browsing	***Proxy***	***VPN***	***Access Routers***
Definition	"Incognito" in Google Chrome "Private Browsing" in Firefox "InPrivate Browsing" in Internet Explorer	prevent the destination from logging IP address and other relevant information of Internet user	Virtual Private Network encrypts all of the packets sent out from users to VPN server.	A random path consisting of multiple nodes are selected, and original data are encrypted and re-encrypted using the public key of the selected nodes.
Pros	Cleans browsing cookies	Hide user's relevant data from the final destination.	all packets that are sent out from the user are encrypted	Use asymmetric cryptography and multiple layers of encryption
Cons	Disclosed by real time attacks as the cleaning is done after the browser is closed.	Disclosed by ISP or an attacker along the route to ISP using traffic analysis	Disclosed by obtaining the secret key or if a VPN server gets hacked	Disclosed by sniffing traffic at the exit node
Anonymity assessment testing	0% Pass	25% Pass	50% Pass	75% Pass
Dynamicity and path changing	Do not support	Do not support	Limited	Support
Cost	Free	Low cost	High-cost	Free
Anonymous Level	Low	Better	Best	High

II. RELATED WORK AND BACKGROUND

Users are very interested in having privacy over all their data, so only their service provider is able to have access to their data. Therefore, Virtual Identity is becoming more and more important for anonymous communication on Internet environment since it can protect people's rights to online privacy even from their service providers.

This section is divided into two parts; the first one presents a review identity categories in social networks, real and cloud environments. In the second part, identity challenges and work motivations is introduced, in addition to, extraction and analysis of an online survey with some questions about using identities in social networking and virtual environments [2].

A. Identity Categories

Two identity categories are discussed:

1) Identity in Social Networks: Undoubtedly, the online social networks (OSNs) became the most visited websites on Internet, with almost one third of all daily online users' transactions visiting them. Non-anonymity communications in social networking platforms disclose privacy. Moreover, users cannot express opinions more freely. In addition, non-anonymity can turn the Internet into a horrible platform because of its built-in nature which making the Sybil attack [3] is piece of cake due to users' identities became easily traceable.

According to the 2015 data breach investigation report [4], threat resulted of social engineering attack is increasing dramatically due to the continually progress in the use of social networking platforms by ordinary and non-technical people, as shown in the Figure 1:

Recently, the most visited online social networks at all, is Facebook that has grown to become one of the most popular social networking platform in the world.

Fig. 1. Number of Breaches per Threat Action Category

It is not only used by many peoples to communicate and share information, but also it turned to be a productive marketing and advertising channel for lots companies, retailers, business entities. In June 2013, there were approximately 1.15 billion monthly active Facebook users [5]. Therefore, Facebook has turned out to become a high-potential target for cyber criminals.

Anonymity on Internet especially on social networks should help users to protect their privacy from getting disclosed. Numerous anonymity techniques are available and used by many technical users on Internet. First of all most of Internet browsers have added anonymous mode to their browsers such as "Incognito" in Google chrome, "private browsing" in Firefox and "InPrivate Browsing" in Internet explorer. Although, the anonymous browsing cleans cookies after the browser is closed, many tools can capture the cookies and use them for real time attack. Another available and widely used anonymity technique is the proxy server, which prevent the server side from logging real IP address of client.

Despite of the client hiding the IP address from target destination, the IP address is still disclosed to the Internet Service Provider (ISP). Therefore by using traffic analysis attacker can get the private information. To solve the proxy server problem, Virtual Private Network (VPN) was introduced to encrypt all of the packets sent from the client. This technique satisfies a higher level of security. There is no chance to decrypt the packets until the VPN server gets hacked. Furthermore, The Onion Router (TOR) is used as the ideal solution for anonymous communication in social networks. This solution has multiple encryption layers and employs asymmetric cryptography. Later, professional attackers pointed out certain vulnerabilities of TOR at exit node; As a solution, TOR uses dynamic IP address to prevent continuous monitoring of exit node [1]

Many works have employed trust in social networks to enhance system anonymity, one of the earlier approaches is [6], which uses personal digital certificates issued by a trusted certificate authority. Then, it applies certain technique such as idemix to make the certificates anonymous, un-linkable, and non-transferable. Consequently, many researches were conducted in this field such as [7-13]. In [14] authors Introduced faceTrust which provide light weighted, flexible and relaxed identity attribute credentials in online social networks. The work in [15] proposed an identity-based Strong Designated Verifier Signature (SDVS) scheme that resists to the key-compromise attack.

2) Identity in Real Time Environment: Identity management using traditional model of username and password became insecure at Internet-scale. The website Experian [16] stated that, in average, the user today shares just five passwords for 26 online identities. Therefore, the problem "break once, break everywhere" arises significantly. Mark Burnett in "10000 Top Passwords" stated that approximately 23% of passwords appear on the table of the three most commonly used passwords as in Table II [17].

Increased security vulnerabilities and growing user frustration have prompted a list of alternatives such as tokens, multi-factor authentication, mutual authentication, biometric identification, and federated identity.

TABLE II. MOST-USED ONLINE PASSWORDS

Frequency	Password
4.7%	password
8.5%	password or 123456
9.8%	password, 123456 or 12345678

Tokens are physical devices generating randomized code that can be used to assure the identity of the user or service which has control of them. Tokens provided by way of either hardware or software, an extremely high level of satisfied authentication because of the multiple exchanges they employ to verify the identity of the user.

Multi-factor authentication approaches intensify security by combining multiple factors: something known (such as a password, PIN) with something we have (such as a token, smart card) with something owned (such as a biometric: retina, hand) and / or something we do (such as voice, handwriting).

Mutual authentication is a model where both the source and the destination entity must fully identify themselves before communication is allowed. It may be accomplished in a number of ways: Diffie-Hellman (DH) key exchange can be used, it provides a more secure method of message exchange and protects the secret being used for an authentication process. This method has a weak point which is the Man In the Middle attack MITM. The solution can be the use or pre-shared key or certificate to avoid this attack. Another method that may be used for mutual authentication is using certificates. The Certificate Authority (CA) must be known by parties to both parties to verify the identities at both sites, and the public keys for both must be shared from the trusted CA.

Biometric identification provides a higher level of authentication than other techniques. It may be used as a main factor of multi-factor authentication, or on a standalone basis. Biometric signatures include fingerprint, iris pattern, facial recognition and heartbeat. Fingerprint-based technology became featured in laptops from manufacturers such as HP, Lenovo and Sony. ING Direct Canada, an online bank, has issued customers with computer mice equipped with fingerprint recognition system. Later, Apple's added fingerprint feature to the iPhone 5S.

Federated identity approaches enable the existing online accounts to be used to sign into new authenticated-access websites (single sign on). Facebook and Google have moved to leverage their vast user-bases to offer such "federated authentication" services. More details about federated identity are presented in Section 3.

Three case studies of trusted service providers such as financial institutions, governments and mobile operators are discussed hereafter. They are well-placed to offer the importance of identity management services for providing the high-security and high-reliability authentication [18]:

a) Financial Institutions: Financial institutions around the world recognized the risk in online transactions where the parties never meet. Therefore, they must rely only upon electronic identity credentials. IdenTrust is the global leader in trusted identity solutions, applied in more than 170 countries, recognized by global financial institutions, government agencies, and commercial organizations around the world [19]. Also, Mint.com, offers personal financial services and credit monitoring, depending on centrally-authenticated access to all of a user's online bank and credit card accounts to collect transactions and balance information across the user's financial issue.

b) Government: Germany, Italy, Spain, Pakistan and Morocco Governments have applied the Electronic Identity Card or "eID" format: a physical identity card with embedded microchip. This approach allows both virtual and physical authentication. The world's first electronic parliamentary elections were held in Estonia in 2007, powered by the Estonia eID card. The European Union's "STORK" program ("Secure idenTity across boRders linked") is working towards a "digital single market by 2015", allowing recognition of national electronic identity (eID) across the European single market. The Netherlands' "DigiD" service now provides single-

password to access over 500 local and national public service organizations, while the US government is working to allow all federal services to be accessed by passwords from approved third parties, such as Google or PayPal, through the "Federal Cloud Credential Exchange" program.

c) Mobile Operators and Manufacturers: The Subscriber Information Module (SIM) allows Mobile Network Operators (MNOs) to authorize access to services, providing a crypto-graphically-protected unique identifier for each user. Turkish operator "Turkcell" charges 5 Turkish Liras (£1.56, or $2.74) per month for its "Mobil imza" application, which it launched in 2007 to facilitate secure, legally-binding consumer and enterprise transactions. Not only MNOs and MVNOs able to take advantage of mobile identity but also the latest smart phones which contain an embedded secure element, providing SIM-like security, beyond the control of the MNO. This creates opportunities for Mobile Operators and Manufacturers like Apple, Google, Samsung and Microsoft to develop wider Identity Management capabilities.

III. Identity in the Cloud & Virtual Environments

In the Cloud Computing Technology Roadmap, the National Institute of Standards and Technology (NIST) highlighted this concern: "… the need for trusted identities, secure and efficient management of these identities while users' privacy is protected is a key element for the successful adoption of any cloud solution." [20].

The best way to address these concerns is to deploy identity management processes and technologies to ensure that only authorized users have access to cloud applications.

Identity Management process depends on two concepts the first one is Single Sign-On (SSO) and the second one is Federated Identity Management (FIM). SSO makes it possible for a user to log in once and gain access to numerous systems or networks available in a federation without being prompted to log in again [21,22].

Federated identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across different autonomous security domains. Consequently, users of one domain can access to all the services offered by another domain without burdening them. Hence, with suitable FIM, users should be able to access data across different domains. One important approach in identity management is the Identity Meta-systems, which is defined as an "interoperable architecture for digital identity that enables people to have and employ a collection of digital identities based on multiple underlying technologies, implementations, and providers" [23].

Numerous identity and federation manager products that support federation via Security Assertion Markup Language (SAML) versions 1.1 and 2.0 are available. Actually, there are three major protocols for federated identity: SAML, OpenID and OAuth. SAML [20] [24] is deployed in SSO systems, large enterprises, government agencies and service providers as their standard protocol for communicating identities across the Internet. SAML is an eXtensible Markup Language (XML) based standard for exchanging authentication and authorization Simple Object Access Protocol (SOAP) messages between security domains, that is, between an identity provider and a service provider. In [25] authors introduced an in-depth analysis of 14 major SAML frameworks and showed that 11 of them, including Salesforce, Shibboleth, and IBM XS40, have critical XML Signature Wrapping (XSW) vulnerabilities.

OpenID is used to implement federated identity management in many web sites like Facebook, Microsoft, Google, PayPal, Symantec, and Yahoo. OpenID is an open, decentralized user identification standard, permitting users to log onto different services with the same digital identity. In OpenID the user is authenticated using third-party services called identity providers through simple URL. Users can choose their preferred identity providers to log onto websites that accept the OpenID authentication scheme. OpenID has some vulnerabilities like Phishing Attacks and Authentication Flaws.

OAuth is the third major open standard protocol for federated identity. OAuth is being used exclusively for authorization purposes and not for authentication purposes like OpenID and SAML. OAuth 2.0 relies entirely on the underlying Secure Socket Layer/Transport Layer Security (SSL/TLS) to provide confidentiality and integrity and does not support signature, encryption, channel binding, and client verification. Therefore, it is described as an inherently insecure protocol.

Finally, there is a growing number of other federated identity approaches.

Higgins, is a new open source protocol that allows users to control which identity information is released to an enterprise or with diverse identity management systems.

Windows U-Prove, is Microsoft new identity meta-system controlled by users, that provides interoperability between identity providers and relying parties.

MicroID, is a new identity layer to the web and micro-formats that allow anyone to simply claim verifiable ownership over their own pages and content hosted anywhere.

Liberty Alliance [26], is a large commercially oriented protocol providing inter-enterprise identity trust. It is the largest existing identity trust protocol deployed around the world.

SXIP [26], is commercially available product that offers users the ability to control their own identity information and authentication in use with blogs and other applications.

INames [26], a new service offering a centralized user controlled identity data store as well as providing authentication trust between enterprises.

OpenSSO, is a Sun Microsystems open source version of their commercial product OpenSSO Enterprise. Shibboleth is a distributed web resource access control system that permits federations to communicate together for sharing web-based resources. It is an open source project that uses OpenSAML toolkit.

Lastly, the Ping Identity [27], Next Generation Identity platform facilitates trusted interaction among groups of

application providers and consumers on the Internet, through APIs, and from any mobile or desktop screen. Regardless of which product is selected, as long as it conforms to the standards of SAML, all products can be used interchangeably with no compatibility issues.

A. Identity Challenges

It is convenient to use a different Virtual Identity V_{ID} for each service. In that way, each V_{ID} is only exposed meanwhile it is used to access to its associated service and it only contains the required attributes for accessing to one service (so less attributes are exposed in a single access to a service).

Furthermore, V_{ID} should be a string that does not include any information about user identity, terminal being used, or service to be accessed. On that way, any sniffer attacker in the access network is only able to know the home domain of the user, but no other information.

It is desirable to maintain a matching between identifiers and services into a private repository, in order to generate the "identity specific side" of V_{ID} in a pseudo-random way. The values stored in this local repository must be maintained equals to the ones in SAML authority side.

B. Work Motivations

1) Analysis of Work Motivations: It is clear that using Identity has been changed over the years; nowdays, we find that all services offered over Internet impose using identities. In addition, each required service enforces users to remember an identity for each one. Another one proposes one identity for all services which is not practical. Therefore, using a new kind of identity will overcome the main issues related to having many identities or one single Identity for all services. Also, the traceability of main identities is reduced as the use of virtual ones cannot lead to the original identity.

In order to extract and analyze these work motivations, we did an online survey composed by questions about using identities in social networking and virtual environment [2]. Then, we compared our proposed mechanism with some existing methodologies to evaluate its performances.

a) Survey Analysis: The results of the survey are used to extract some directives to be used in developing/proposing a new solution that enables personalized Identity for services, mapping Identity to user or service's needs. Through this questionnaire [2], there are a series of questions used to assess user requirements & user satisfactions and to suit their needs from using Identity over social & virtual environments. Moreover, users are asked users to answer some relevant questions about service virtualization knowledge and their identities while accessing social networks like YouTube, Facebook, or Dailymotion. The answer's investigation revealed the existence of two types of user: users from inside the National Telecommunication Institute (Egypt) [28] and users from outside. The participants in this of this survey are mainly scientific users and the institute colleagues' staff. Therefore, their's culture played an important role in the questionnaire answers and overall analysis. The survey has some direct questions about using new Internet services if the access to them needs some personal qualifications. Actually, the major of this survey was to ask about identity and its privacy. Therefore, the following two sections describe the most important points in the results' analysis.

b) Knowledge and Identity Use: All target users have a good knowledge about social networking access (as the survey indicated 100%). Among them, about 70% prefer using one main identity for all online social sites by means of creating one identity for each service automatically by the operators as shown in Figure 2. By this, the users are searching for an easy solution in order to avoid remembering many identities for all services.

c) Privacy and Virtual Identity: The need for privacy and virtual identity for users is investigated through YES/NO questions. Figure 3 illustrates some questions samples and the answers globally indicate 70% of users are interested in privacy and virtual identity aspects.

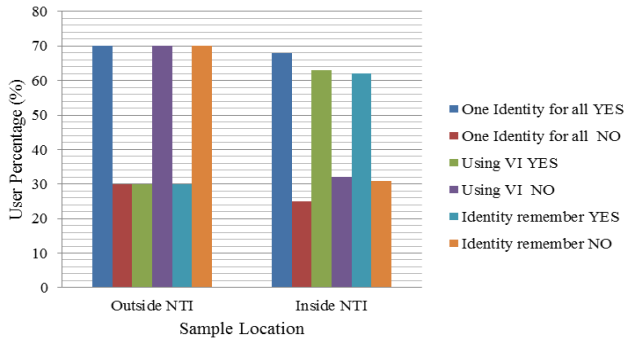

Fig. 2. Identity background questions/answers in the online survey

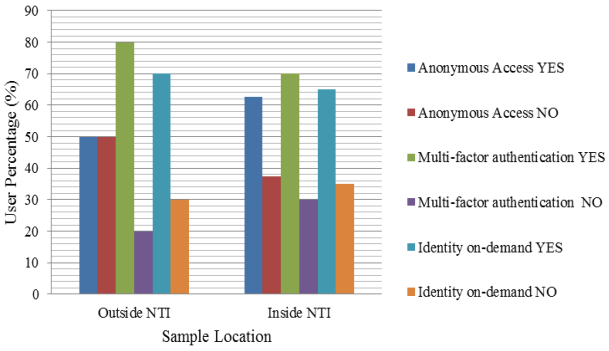

Fig. 3. Identity security and privacy questions/answers in the online survey

2) Survey Conclusion: This survey leads to the major conclusion, which is the importance of using V_{ID} in social environment. The users are motivated to use this principle of access and searched for more privacy by asking for this technique.

IV. Proposed Virtual Identity Mechanisms

In this work, we introduce the IBE and PBE as two approaches for generating virtual identities by collaboration with the Private Key Generator (PKG). The PKG is the security server which is used to generate the IDs deployed in cloud

service access based on the type of service required by cloud's user as shown in Figure 4.

Two secure mechanisms for creating V_{ID} are proposed (one based on IBE and the other based on PBE); they are mainly using public-key cryptography for encryption and digital signatures. The key length for most used public key cryptography algorithms has increased over recent years, and this has put a heavier processing load on applications using these algorithms. This burden has ramifications, especially for social and commerce sites that conduct large numbers of secure transactions. Thus, Elliptic Curve Cryptography (ECC) is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography. The principal attraction of ECC, compared to others, is that it appears to offer equal security to RSA for a far smaller key size, thereby reducing processing overhead [29]. Therefore, ECC was chosen in the design of the new proposed solutions. The two solutions need a Private Key Generator (PKG) to calculate the V_{ID}. However, these approaches assume that a centralized Trust Authority (TA) is in charge of the private key generation. Thus, the anonymous communications are not anonymous to the TA. Nevertheless, they use different encryption techniques.

We implemented the two mechanisms IBE and PBE using Multi-precision Integer and Rational Arithmetic C/C++ (MIRACL) library [30] to evaluate the feasibility, performance and scalability of the proposed solutions. Figure 5 and Figure 6 show the two algorithms messages exchanges.

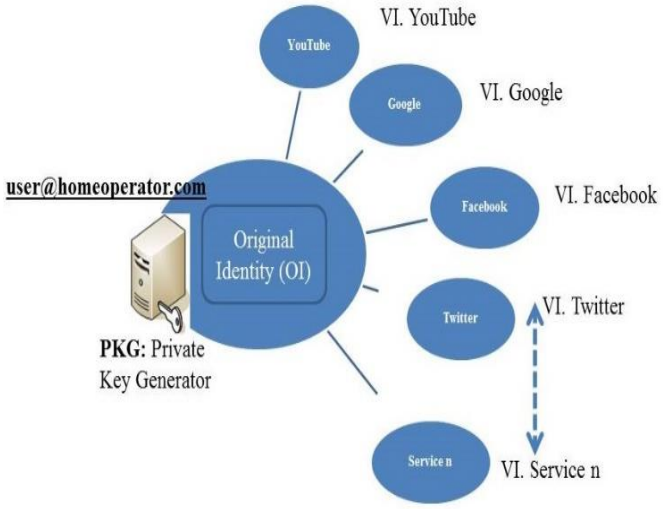

Fig. 4. Virtual Identities generation framework

A. The First Approach using Identity-basedEncryption (IBE)

Public-key based solution, such as Identity-Based Cryptographic (IBC) is an asymmetric key cryptographic technique, in which a user's public key can be an identifier of the user and the corresponding private key is created by binding the identifier with a system master secret [31].

The first approach is based on the IBC, which can be traced back to the IBE firstly proposed by Shamir. The construction of the proposed IBE scheme is shown in Figure 5.

Since we use for this solution IBE and ECC, we have to set up the ECC parameters. The equation of the elliptic curve that we used is $y^2 = x^3 + ax + b \bmod p$. The points of this curve define a finite field; their number must be a prime number. In order to satisfy this condition we used the ECPG algorithm. we fixed a prime number (p) and random integer (a). Then we initialize the variable (b) and calculate (n) (the number of points) on the elliptic curve. We used a function in MIRACL that can calculate the number of the points in a finite field. The principle of the algorithm is as in Table III.

The main steps of the proposed solution are:

a) System setup: Each user send U_{ID}: User ID and Ser: Requested Service to Private Key Generator PKG. The Private Key Generator (PKG) or the trust Authority (TA) selects an elliptic Curve E over GF (p) where p is a big prime number. We also denote P as the generator point of E and q (big number), as the order of P. The master Key X = (x1, x2….xn-1, xn). The public Key Y= (y1, y2…yn-1, yn) where yi=xi*P for i=1: n.

b) Key extraction: Given U_{ID}, Ser. PKG generates V_{ID} The Virtual Identity V_{ID} (V_{ID}=Original identity (mail, service) * Point on elliptic curve).

The User public key UP=H*V_{ID} (H is a secure hash function).

The User private key UD=S*UP (S is the master secret key of PKG).

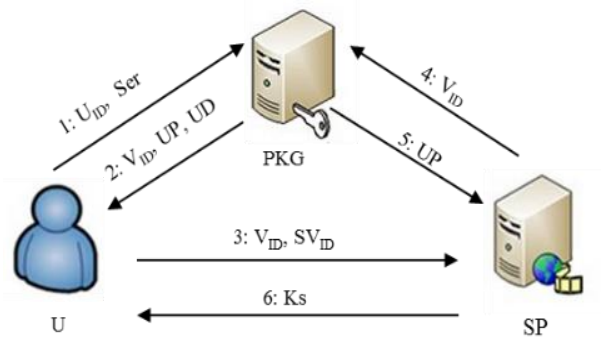

Fig. 5. Proposed IBE Messages Exchanges

TABLE III. ALGORITHM 1 : ECPG ()

Algorithm 1 : ECPG ()
1 : Choose p and a
2 : Initialize b
3 : Calculate n
4 : If n is prime, n will be the proper parameter Else, increase b by 1
5 : Go to 3

c) Signature generation: The announcing user receives V_{ID}, UP and UD from PKG. In order to sign the user virtual identity V_{ID} using a private key UD derived from the PKG to determine V_{ID} and signature SV_{ID}, the announcing user:

- Receives V_{ID}, UP and UD from PKG
- Execute EcdsaSign (V_{ID}, UD) as in Table IV to determine SV_{ID}

TABLE IV. ALGORITHM 2 : ECDSASIGN (V_{ID}, UD)

Algorithm 2 : EcdsaSign (V_{ID}, UD)
1 : Generate n a large prime number
2 : Calculate d= UD mod (n-2)
3 : Computes Q = d* UP
4 : Select a unique and unpredictable integer k in the interval [1, n-1].
5 : Compute k* UP = (x1, y1) and r = x1 mod n. If r = 0, then go to 4.
6 : Compute k-1 mod n.
7 : Compute s = k-1*(h (V_{ID}) + d*r) mod n (h is the Secure Hash Algorithm)
8 : The signature for V_{ID} is the pair of integers (r, s) = Sig (V_{ID}).
9 : Return Sig (V_{ID}) = (r, s)
10 : Publish (Sig (V_{ID}), n, Q)

d) Signature Verification: Once the service provider SP receives the signed virtual identity V_{ID}, it asks PKG for the public key for checking the signed virtual identity SV_{ID}, Algorithm 3 steps are given in Table V.

TABLE V. ALGORITHM 3: ECDSAVER (V_{ID}, UP)

Algorithm 3 : EcdsaVer (V_{ID}, UP)
1: Verify that r and s are integers in the interval [1, n-1].
2: Compute w = s-1 mod n and h (V_{ID}).
3 : Compute h(V_{ID})*w mod n and r*w mod n
4: Compute h(V_{ID})*w mod n*UP + r*w mod n*Q = (x0, y0), v = x0 mod n.
5 : Accept the signature if and only if v=r.

e) Encrypt future communication: If the verification of the signature is successful, the service provider SP generates Shared Secret Key Ks and sends it to user U. Otherwise Ks is discarded. After the generation of the pre-shared key Ks, the future messages are encrypted using pre-shared key Ks as EcdhEncrypt (m), Algorithm 4, Table VI. The resulting ciphertext is denoted by c. The decryption of ciphertext c using the same pre-shared key Ks is given as EcdhDecrypt(c), Algorithm 5, Table VI.

TABLE VI. ALGORITHM 4: ECDHENCRYPT (M); ALGORITHM 5: ECDHDECRYPT (C)

Algorithm 4 : EcdhEncrypt (m)	**Algorithm 5 : EcdhDecrypt (c)**
1 : Gen. random number a ∈ GF (p).	1 : Gen. random number b ∈ GF (p).
2 : Calculate multi_a= a.UP	2 : Calculate multi_b= b.UP
3 : Publish (multi_a)	3 : Publish (multi_b)
4 : Receive multi_b	4 : Receive multi_a
5 : Calculate Ks=a*multi_b	5 : Calculate Ks=b*multi_a
6 : Encrypt m with Ks, {m} Ks	6 : Encrypt m with Ks, {m} Ks
7 : Return c= {m} Ks	7 : Return {m} Ks

B. The Second Approach using Pseudonym Based Encryption

The second approach is based on Pseudonym Based Encryption (PBE), which was proposed for Key management for anonymous communication in mobile ad-hoc networks [32]. In this approach, user uses PBE to calculate its own V_{ID}. The PKG just computes the user's private key, which depends on its secret master key. The PKG will act as an authority that certifies that the user has the private key corresponding to his/her public key. Figure 6 shows the second solution based on PBE messages exchanges.

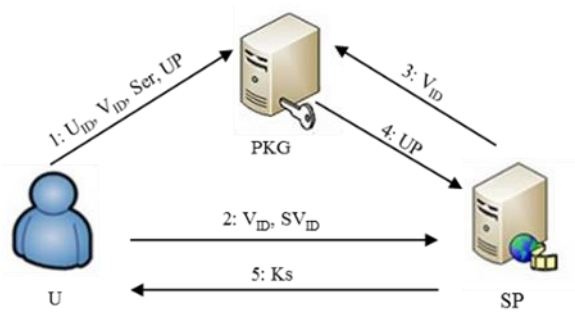

Fig. 6. Proposed PBE Messages Exchanges

The user sends to the PKG his/her identity (e.g., user@homeoperator.com), the requested service, the public key by choosing an elliptic curve with its generator point P and chooses his/her V_{ID} (as pseudonym). The PKG calculates the user's private key UD and doesn't need to send the key pair (public/private) to the user because the UP and UD are already computed by the user. The user wants to be authenticated by SP; therefore, he/she uses an Identity-Based Signature (IBS) [33] to calculate SV_{ID} and sends it with V_{ID} to the SP. The SP sends V_{ID} to the PKG and asks for public key corresponding to the V_{ID}. The SP verifies the SV_{ID} by decrypting it using the UP. If it retrieves the V_{ID}, then the authentication succeeds. At the end, the SP generates and sends a shared secret key to the user to encrypt future communication between them.

We implement the second solution using the same steps as done in the first one except for the second step in IBE (as the trusting is verified by the cloud service provider in this case).

- Each user sends U_{ID}: User ID and Ser: Requested Service V_{ID}: Virtual ID (Pseudonym), UP: User Public Key to Private Key Generator PKG. The PKG is in charge of the private key generation within an anonymous communication system. Therefore, the anonymous communications are not anonymous to the trust authority (TA).
- The PKG/TA just computes the user's private key, which depends on its secret master key. PKG selects an elliptic Curve E over GF (p) where p is a big prime number. The PKG calculates the user's private key UD and doesn't send the key pair (public/private) to the user because the UP and UD are already computed by the user.
- Other steps follow the same way as described before in the first solution.

C. Processing time for IBE and PBE resulting from MIRACL

We used MIRACL Library during the evaluation of our solution's performance to observe the processing time for all functions and executed entities. The results for the two proposed solutions IBE and PBE are illustrated in the following two tables (Table VII and Table VIII).

TABLE VII. PROCESSING TIMES FOR IBE

Message ID	Source	Destination	Depends On	Processing Time (sec)
1	U	PKG	Beginning	N/A
2	PKG	U	ID:1	0.034
3	U	SP	ID:2	0.004
4	SP	PKG	ID:3	0.0015
5	PKG	SP	ID:4	0.0015
6	SP	U	ID:5	0.009
Six messages total				0.05

TABLE VIII. PROCESSING TIMES FOR PBE

Message ID	Source	Destination	Depends On	Processing Time (sec)
1	U	PKG	Beginning	N/A
2	U	SP	ID:1	0.033
3	SP	PKG	ID:2	0.0015
4	PKG	SP	ID:3	0.028
5	SP	U	ID:4	0.009
Five messages total				0.0715

The results we got to calculate the processing times for all messages are around 0.05 Sec and 0.0715 Sec for all executed entities and functions for IBE and PBE respectively, using a computer machine has specs, Intel Core 2 Duo CPU E8400 @ 3.00GHz x 2, memory 4G in Linux Ubuntu 12.10. Table VII and VIII show the processing times for IBE and PBE as captured during the two scenarios validation.

V. PERFORMANCE EVALUATION USING OPNET MODELER

Optimized Network Performance (OPNET) Modeler [34] is a discrete event simulation tool. It provides a comprehensive development environment supporting the modeling and simulation of communication networks. This contains data collection and data analysis utilities. OPNET allows large numbers of closely spaced events in a sizeable network to be represented accurately. This tool provides a modeling approach where networks are built of nodes interconnected by links. Each node's behavior is characterized by the constituent components. The components are modeled as a final state machine. Actually, we used Application Characterization Environment (ACE), which is included in OPNET Modeler to visualizes, analyzes, and troubleshoots networked applications.

A. Network Model Scenarios

ACE has a number of predictive features that enable us to determine how network and application changes will affect application performance. Therefore, we used it to evaluate the proposed solutions. First, we use ACE whiteboard to draw exchanging messages among the three entities User (U), Private Key Generator (PKG) and Service Provider (SP). Therefore, we set the processing time for each message as obtained from MIRACL validations. After that, from the ACE whiteboard, we draw the two scenarios of network topology for each proposed solution. The first scenario is for local clients and the second scenario is for remote clients. For each proposed solution we evaluated the performance in two cases, the first one is when clients (users) need single service and the second one is when users need more than one service access (exactly ten services). Finally, we compared the results obtained and conclude this performance evaluation.

B. Simulation Results

As shown in the following sections, we implemented four different scenarios. In all scenarios, we measured the application response time, which is described as the time taken for all the tasks in the custom application to complete.

1) First solution using IBE with Single Service: As shown in Figure 7, the application response time is not zero for all users. Nevertheless, it has small values such that the application response time resulted when one user used one service is 0.052857 seconds and when 200 users used one service is 0.406446 sec. We noticed the differences when remote users use one service.

2) First solution using IBE Multiple Services: Application response time increased when users used many services. Actually, we simulated 10 services for each user. Figure 8 highlights the two use cases of accessing either locally or remotely for multiple services (10 services) IBE virtual identity-basedgeneration.

3) Second solution using PBE Single service: As shown in Figure 9, the values of application response time that we got close to the values mentioned earlier in the case of IBE single service. As mentioned before, these values are not zero but the application response time resulted when one user used one service is 0.075512 seconds and when 200 users used one service is 0.406088 sec. We noticed the differences when remote users use one service.

4) Second Solution using PBE Multiple Services: As mentioned before, application response time increased when cloud users requested many services. We note that, PBE application response time is better than IBE application response time when using users multiple services scenario as it is clear in Figure 10.

5) Global Results: We note the difference when remote users used many services. In fact the scenario of remote users multiple services is the actual one. Most cloud users used many services remotely. Therefore, we can emulate the number of users and application response time resulted from this scenario to calculate the overall delay for actual cloud networks used IBE to create V_{ID} for anonymous communication.

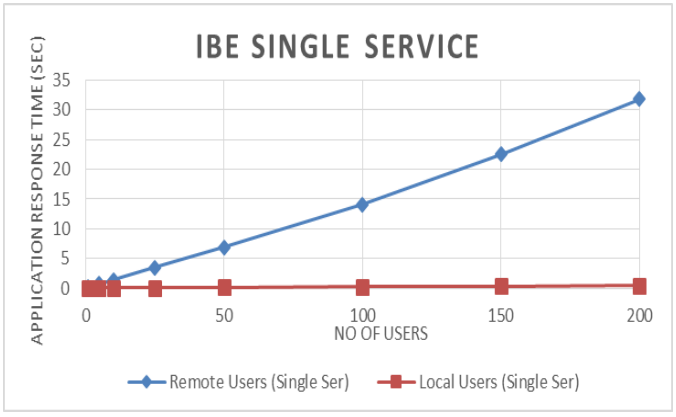

Fig. 7. IBE Single Service

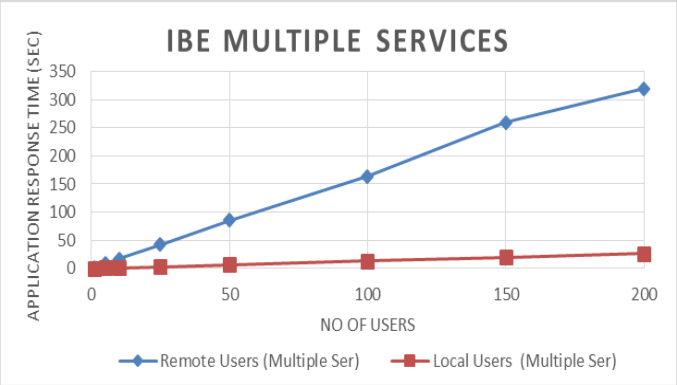

Fig. 8. IBE Multiple Services

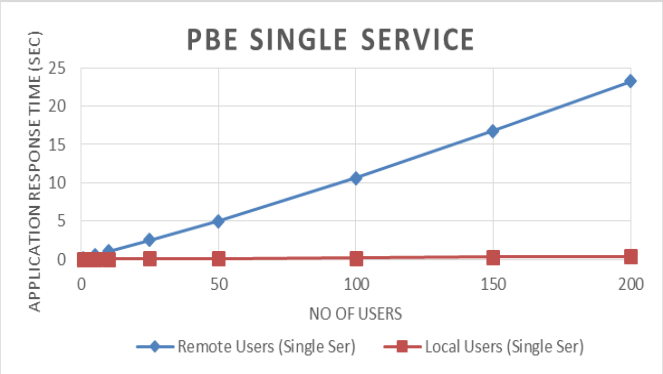

Fig. 9. PBE Single Service

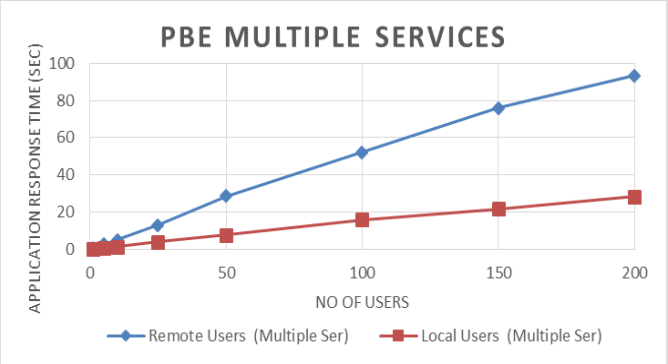

Fig. 10. PBE Multiple Services

VI. Conclusions

In cloud computing environment, users want to protect their privacy and their identities. In the literature, different manners to use identities in the network application are found. In this paper, two novel approaches to generate virtual identities are proposed. The first one is based on the Identity Based Encryption (IBE) and the second one, on Pseudo Based Encryption (PBE). We started by complete study about the identity management in general and the virtual identity in particular. Then, and in order to validate our work motivations, an online survey about issues and opportunities in virtual environment is analyzed to draw our framework architecture for supporting VID solutions. The proposed solution defined a single sing on and anonymous communication to help Cloud and Internet users protecting their privacy and private information from any disclosure. Both approaches implementations are validated using MIRACL library. Furthermore, another performance evaluation is done using OPNET Modeler. The evaluation drew our attention through the proposed solutions feasibility in cloud scale applications or services based on simulating single and multiple services for both local and remote users access. As future directions for this work, we will validate our solutions in a real cloud platform like OpenStack in correlation with keystone security server for best integration with cloud scalability.

References

[1] Hoang N., and Pishva D., "Anonymous Communication and its Importance in social networking", ICACT2014, February 16-19, 2014.

[2] Survey about using Identities in Social Networks and Virtual Environments, http://www.ntiegypt.sci.eg/survey/index.php/212212/, last visit: December, 2015.

[3] Danezis G. and Mittal P., "Sybil Infer: Detecting Sybil Nodes using Social Networks", NDSS, 2009.

[4] Threat Actions, the 2014 data breach investigations report, Verizon enterprise, page 9, http://www.verizonenterprise.com/DBIR/2015/, last visit: December, 2015

[5] Facebook reports second quarter 2013 results, Facebook, Retrieved 24 July 2013.

[6] Camenisch J. and Herreweghen E., "Design and Implementation of the idemix Anonymous Credential System", ACM CCS, 2002.

[7] Pujol J. and Delgado R., "Extracting Reputation in Multi Agent Systems by Means of Social Network Topology", AAMAS, 2002.

[8] Sovran Y., Libonati A., and Li J., "Pass it on: Social Networks Stymie Censors", IPTPS, 2008.

[9] Ramachandran A., and Feamster N., "Authenticated Out-of-Band Communication over Social Links", WOSN, 2008.

[10] Yardi S., Feamster N., and Bruckman A., "Photo-Based Authentication Using Social Networks", WOSN, 2008.

[11] Tran D., Min B., Li J., and Subramanian L., "Sybil-Resilient Online Content Rating", NSDI, 2009.

[12] Lesniewski-Laas C. and Whanau M., "A Sybil-proof Distributed Hash Table", NSDI, 2010.

[13] Post A., Shah V., and Bazaar A., "Strengthening user reputations in online marketplaces", NSDI, 2011.

[14] Sirivianos M., Kim K., Gan J. and Yang X., "Assessing the veracity of identity assertions via OSNs", IEEE, 2012.

[15] Lin H., "Toward Secure Strong Designated Verifier Signature Scheme from Identity-Based System", IAJIT, Vol.11 No.4, July 2014.

[16] Experian, http://press.experian.com/, last visit: December, 2015.

[17] Burnett M., "10,000 Top Passwords", https://web.archive.org/web/20150315000117/ https://xato.net/#.Vm2Zs0p97IV, last visit: December, 2015.

[18] Dargue M. and Wadsworth W., "Cartesian: Identity in the Internet Age" the management network group, September 2013.

[19] IdenTrust: Bank Assurance for Government, White Paper, IdenTrust Inc., USA.

[20] National Institute of Standards and Technology (NIST), Computer Security Division, Information Technology Laboratory, July 2013.

[21] Galpin R. and Flowerday S., "Online Social networks: Enhancing user trust through effective controls and identity management", IEEE, 2011.

[22] Hamlen K., Liu P., Kantarcioglu M., Thuraisingham B. and Yu T., "Identity Managemnet for Cloud Computing: Developments and Directions", CSIIRW '11, October 12 -14, 2011.

[23] Lewis K. and Lewis J., "Web Single Sign-On Authentication using SAML", IJCSI, Vol. 2, pp.41-48, 2009.

[24] Prasanalakshmi B. and Kannammal A., "Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics", International Journal of Computer Applications, Volume 53, No.18, September 2012.

[25] Somorovsky J., Mayer A., Jorg S., Schwenk j., Kampmann M., and Jensen M., "On Breaking SAML: Be Whoever You Want to Be", 21st USENIX Security Symposium, August 8-10, 2012.

[26] Authentication world, http://www.authenticationworld.com/Authentication-Federation, last visit: December, 2015.

[27] Ping Identity, https://www.pingidentity.com/en/products/next-gen-identity.html, last visit: December, 2015

[28] National Telecommunication Institute, http://www.nti.sci.eg/, last visit: December, 2015

[29] Stallings W., Cryptography and Network Security: Principles and Practice, 5/E, Prentice Hall, 2011.

[30] Multi-precision Integer and Rational Arithmetic C/C++ (MIRACL) library, http://info.certivox.com/, last visit: December, 2015.

[31] Chen L., "An Interpretation of Identity-Based Cryptography", Foundations of Security Analysis and Design IV, Lecture Notes in Computer Science, Volume 4677, 2007.

[32] Huang D., "Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks", Int. J. Security and Networks, Vol. 2, 2007.

[33] Boneh D. and Franklin M., "Identity-Based Encryption from the Weil Pairing", CRYPTO 2001, LNCS 2139, Springer-Verlag, 2001.

[34] Riverbed, http://www.riverbed.com/, last visit: December, 2015.